RANSOMWARE & RANÇONGICIELS

1er décembre 2016

Colloque sur le cyber et les collectivités territoriales
Chaire Cybersécurité & Cyberdéfense

Francois Paget
Chercheur en cybercriminalité

ADHÉRENT CLUSIF 2016

Ransomware / Rançongiciels

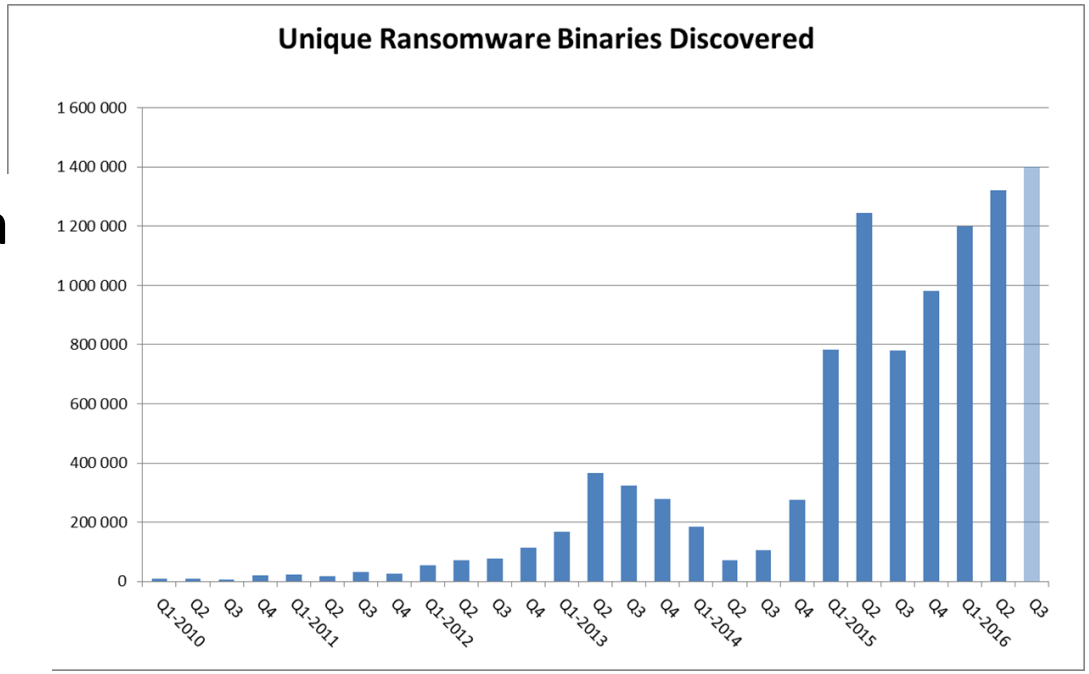
Sommaire

- Définition
- Cibles
- Auteurs et rançons
- (Historique)
- Vecteurs d’infection et prévention
- En cas d’infection

Ransomware / Rançongiciels

Définition

- Successeurs des faux anti-virus (en anglais, *scareware*).
- Programmes malveillants qui paralysent le système d'information de leurs victimes puis réclament une rançon pour le rétablir.
  - Rançongiciels bloquants,
  - Rançongiciels chiffrants,
- Paiement à effectuer en monnaie virtuelle ou cartes prépayées,
- Respect des d'engagements par les escrocs.



Source McAfee Labs / François Paget (juillet 2016)

Ransomware / Rançongiciels

Leurs nouvelles cibles : les entreprises, les administrations avec, en infraction au « code d'honneur », une attrait pour les services de santé

Date	Hôpitaux
6 janvier 2016	États-Unis, Texas
6 janvier 2016	États-Unis, Massachusetts
6 janvier 2016	Allemagne
6 janvier 2016	Australie
19 janvier 2016	Australie, Melbourne
3 février 2016	Royaume-Uni
3 février 2016	Corée
3 février 2016	États-Unis
12 février 2016	Royaume-Uni
12 février 2016	États-Unis
27 février 2016	États-Unis, Californie
5 mars 2016	Canada, Ottawa
16 mars 2016	États-Unis, Kentucky
18 mars 2016	États-Unis, Californie
21 mars 2016	États-Unis, Géorgie (cabinet dentaire)
22 mars 2016	États-Unis, Maryland
28 mars 2016	États-Unis, Maryland
29 mars 2016	États-Unis, Indiana
31 mars 2016	États-Unis, Californie
16 mai 2016	États-Unis, Colorado

Ransomware au Centre Hospitalier d'Epinal

Diffusé le 02 Mar 2016 Par : Damien Bancal Commentaire : 0 Tag: Dridex, hopital, medecin, ransomware

On a beau en parler en long et en travers, le ransomware, le rançonnage informatique, n'a pas fini de faire des dégâts. Un médecin Français a cliqué sur un fichier joint dans un courriel usurpant un avocat. Un serveur de son hôpital pris en otage.

http://www.zataz.com/ransomware-centre-hospitalier/#axzz4QLd6B6lM/

Source McAfee Labs (juillet 2016)

Ransomware / Rançongiciels

Leurs nouvelles cibles : les collectivités territoriales aussi !

Après quatre ans d'utilisation, la Mairie de Marsannay-la-Côte
sa confiance à

Le 24 mai 2016

Commune de plus de 5000 habitants faisan
de Marsannay-la-Côte compte une centaine

www.sudouest.fr/2016/05/11/des-hackers-reclament-une-rancon-a-la-mairie-2358354-3827.php

Google !Search !System Achats Actu Divers Encyclo_gen Perso Drone Ecoute

Lot-et-Garonne : des hackers piratent le site d'une mairie et réclament une rançon

Publié le 11/05/2016 . Mis à jour à 12h36 par Blandine Philippon

Mairies françaises attaquées par un ransomware russe

Diffusé le 23 Jan 2015 Par : Damien Bancal Commentaires: 2 Tag: Critoni, ctb, locker, mairie, ransomware

Retour du ransomware CTB. Étonnant, la cochonnerie numérique a touché lundi plusieurs mairies Françaises.

ZATAZ.COM a appris qu'une étonnante attaque a visé plusieurs mairies françaises. Lundi 19 janvier, les ordinateurs de collectivités locales comme la ville de Fontenay-le-Comte (les autres mairies ont demandé à zataz.com de ne pas être citées, ndr) ont été prises pour cible par un courrier piégé.

Ransomware / Rançongiciels

Les paiements se multiplient

...que les cybercriminels convoitent leur argent, sachant que les victimes paieront...

La moitié des victimes se disent prêtes à payer près de 500 € pour récupérer leurs données, même si les cybercriminels pourraient ne pas leur fournir la clé de déchiffrement ou leur demander une somme supplémentaire, notamment pour développer de nouveaux outils.

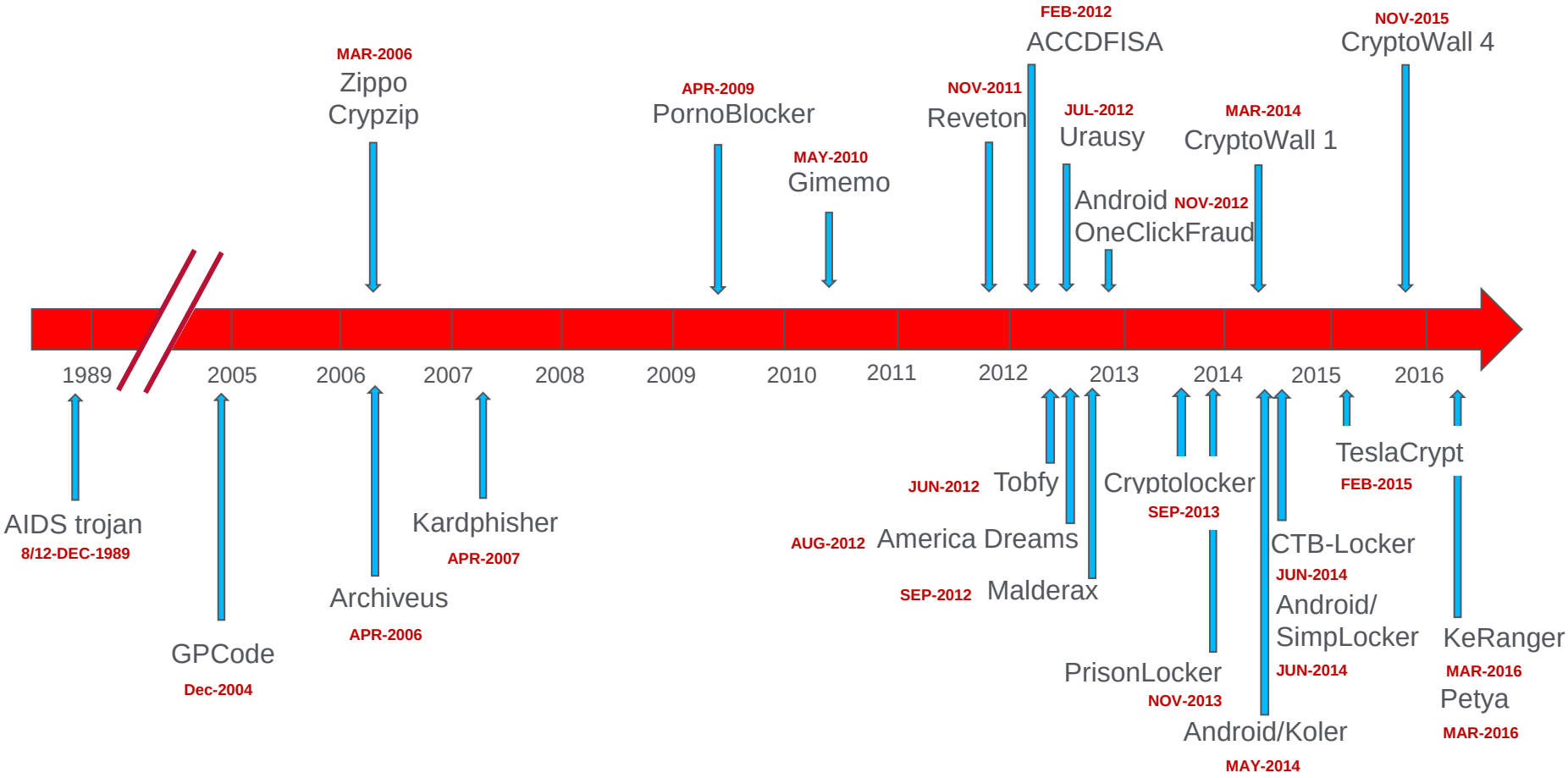
Pays	Victimes ayant payé	Victimes prêtes à payer
États-Unis	50%	40%
Allemagne	33%	36%
Roumanie	48%	52%
France	N/A	32%
Royaume-Uni	44%	31%
Danemark	30%	14%

Transactions		
No. Transactions	50	
Total Received	189,813.81836182 BTC	
Final Balance	148,312.81836182 BTC	

En 6 mois, les auteurs de *« samsam »* annoncent un CA de 121 millions de dollars pour un bénéfice de 94 millions de dollars.

Ransomware / Rançongiciels

Historique



Ransomware / Rançongiciels

Vecteurs d'infection,

- Réception de courriel,
- Exploits de navigateur (ou *drive-by-download*),
- Téléchargements risqués.

Prévention,

- Réfléchir avant de double-cliquer, apprendre à distinguer le vrai du faux,
  - C'est parfois difficile,
- Avoir son système d'exploitation et ses outils bureautique à jour (Adobe Reader, Microsoft Office, etc.),
  - Ne pas activer l'exécution de macros,
- Avoir un navigateur Internet à jour, au même titre que sa suite Adobe Flash ou encore Java,
  - vérifier l'absence d'extension (ou plug-in) douteuse.

Ransomware / Rançongiciels

En cas d'infection…

- Isoler la machine concernée, déconnecter les éventuels disques externes,
- Ne rien effacer, ne rien « nettoyer »,
- Faire une copie de quelques fichiers touchés ; notez leurs noms et leurs extensions,
- Avant d'éteindre, prendre une photo du message qui s'affiche à l'écran.

- Inspecter depuis un PC sain l'état des disques externes et des zones de stockage distant. Sont ils lisibles ?

… ai-je des sauvegardes ????

Ne pas hésiter à contacter votre équipe informatique et/ou votre pôle sécurité

Ransomware / Rançongiciels

(… en cas d'infection), j'ai des sauvegardes !

- Tentez d'éliminer le ransomware utilisation de plusieurs anti-virus, etc.),
  - Pour ma part, je conseille plutôt, dès que cela est possible, une réinitialisation totale de la machine.
- Restaurez vos données depuis vos sauvegardes,
- Tentez de définir l'origine de l'infection afin d'éviter sa réapparition.

Ne pas hésiter à contacter votre équipe informatique et/ou votre pôle sécurité

Ransomware / Rançongiciels

(… en cas d'infection), je n'ai pas de sauvegarde

- Définissez avec précision le type et la version du rançongiciel qui vous a atteint,
  - Message, nom des fichiers, base de registres, etc.
  - Une clé pointe sans doute sur le fichier d'informations mis en place par le rançongiciel,
- Recherchez un outil de décryptage,
- Testez-le sur les copies de vos originaux chiffrés que vous aviez préalablement dupliqués,
  - Ne travaillez jamais sur les originaux (chiffrés) afin d'éviter qu'une fausse manipulation ne les détériorent.

Suis-je sauvé ????

Ne pas hésiter à contacter votre équipe informatique et/ou votre pôle sécurité

Ransomware / Rançongiciels

(… en cas d'infection), sans sauvegarde, sans décrypteur

- Vous êtes mal !!!!!!!!!!!!!!!!!!!
  - Soit vous payez, soit vous tirez une croix sur vos données !
- Utilisez la machine sur laquelle la demande de rançon s'est affichée.
  - Prenez soin de reconnecter « en l'état » tous vos supports atteints par le ransomware.
- Vérifier les modalités de paiement, êtes vous dans les délais ? Si tout est OK, payez !
  - Une fois le virement (irrévocable) effectué, vous recevrez sans doute l'accès à un exécutable de déchiffrement ou une clé à entrer directement sur l'écran d'invite. Suivez la procédure, et je l'espère, récupérez vos données.
- révisez vos modes de protections afin de ne pas retomber dans le piège.

Ne pas hésiter à contacter votre équipe informatique et/ou votre pôle sécurité

Ransomware / Rançongiciels

Quel avenir pour les ransomware ?

- Toujours plus de professionnalisme (ne pas tuer la poule aux œufs d'or !),
- Des ransomware ciblants (les collectivités territoriales sont des cibles attractives),
- Des ransomware sur nouveaux médias:
  - IoT (Internet des objets): TV, frigo, montre connectée,
- Des ransomware physique,
  - Isolement du domicile,
  - Blocage du véhicule,
  - Chantage médical.